Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) In a computing device, a method for protecting sensitive files from unauthorized access, comprising:

detecting a connection of the computing device to an electronic device;

accessing an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type;

determining whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

accessing sensitive file information which identifies multiple sensitive files stored on the computing device, wherein the sensitive files are not identified until after the connection has been identified as not being in the authorized connection list, wherein the sensitive file information is separate from the sensitive files; and

preventing access to all of the sensitive files identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list, wherein the sensitive files continue to be stored on the computing device but all of the sensitive files cannot be accessed when access is being prevented.

2. (Previously Presented) The method of claim 1, wherein if the connection is not identified in the authorized connection list the method further comprises:

detecting termination of the connection; and

if the computing device does not have any other unauthorized connections, restoring access to the sensitive files identified by the sensitive file information.

3. (Original) The method of claim 1, wherein the connection occurs via a computer network.

4. (Original) The method of claim 3, wherein the network is a wireless network, and wherein the computing device is a mobile computing device.

5. (Original) The method of claim 1, wherein the connection is a direct connection.

6. (Previously Presented) The method of claim 1, wherein the access prevention task comprises locking the sensitive files.

7. (Previously Presented) The method of claim 1, wherein the access prevention task comprises encrypting the sensitive files.

8. (Previously Presented) The method of claim 1, wherein the computing device comprises a storage device, and wherein the access prevention task comprises moving the sensitive files to a host-protected area of the storage device.

9. (Previously Presented) The method of claim 1, wherein the sensitive file information is a reference to a directory in which at least one of the sensitive files is stored.

10. (Previously Presented) The method of claim 1, wherein the sensitive file information is a list of the sensitive files.

11. (Canceled)

12. (Canceled)

13. (Currently Amended) In an administrative system which distributes software to a plurality of computing devices on an enterprise network, a method comprising:

providing a security agent, wherein after installation on a computing device the security agent is configured to:

detect a connection of the computing device to an electronic device;

access an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type;

determine whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

access sensitive file information which identifies multiple sensitive files stored on the computing device, wherein the sensitive files are not identified until after the connection has been identified as not being in the authorized connection list, wherein the sensitive file information is separate from the sensitive files; and

prevent access to all of the sensitive files identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list, wherein the sensitive files continue to be stored on the computing device but all of the sensitive files cannot be accessed when access is being prevented; and

transmitting the security agent to the plurality of computing devices via the enterprise network.

14. (Original) The method of claim 13, further comprising:

providing the authorized connection list;

providing the sensitive file information; and

transmitting the authorized connection list and the sensitive file information to the plurality of computing devices via the enterprise network.

15. (Currently Amended) A computing device that is configured for protecting sensitive files from unauthorized access, comprising:

a processor;

memory in electronic communication with the processor; and

instructions stored in the memory, the instructions being executable to:

detect a connection of the computing device to an electronic device;

access an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type;

determine whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

access sensitive file information which identifies multiple sensitive files stored on the computing device, wherein the sensitive files are not identified until after the connection has been identified as not being in the authorized connection list, wherein the sensitive file information is separate from the sensitive files; and

prevent access to all of the sensitive files identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list, wherein the sensitive files continue to be stored on the computing device but all of the sensitive files cannot be accessed when access is being prevented.

16. (Previously Presented) The computing device of claim 15, wherein if the connection is not identified in the authorized connection list the instructions are further executable to:

detect termination of the connection; and

if the computing device does not have any other unauthorized connections, restore access to the sensitive files identified by the sensitive file information.

17. (Previously Presented) The computing device of claim 15, wherein the access prevention task comprises at least one of locking the sensitive files, encrypting the sensitive files, and moving the sensitive files to a host-protected area of a storage device.

18. (Currently Amended) A non-transitory computer-readable medium for storing program data, wherein the program data comprises executable instructions, the executable instructions being executable to:

detect a connection of a computing device to an electronic device;

access an authorized connection list, wherein the authorized connection list comprises a list of at least one authorized network or a list of at least one authorized connection type;

determine whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

access sensitive file information which identifies multiple sensitive files stored on the computing device, wherein the sensitive files are not identified until after the connection has been identified as not being in the authorized connection list, wherein the sensitive file information is separate from the sensitive files; and

prevent access to all of the sensitive files identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list, wherein the sensitive

files continue to be stored on the computing device but all of the sensitive files cannot be accessed when access is being prevented.

19. (Previously Presented) The non-transitory computer-readable medium of claim 18, wherein if the connection is not identified in the authorized connection list the executable instructions are further executable to:

detect termination of the connection; and

if the computing device does not have any other unauthorized connections, restore access to the sensitive files identified by the sensitive file information.

20. (Previously Presented) The non-transitory computer-readable medium of claim 18, wherein the access prevention task comprises at least one of locking the sensitive files, encrypting the sensitive files, and moving the sensitive files to a host-protected area of a storage device.